

FILED

UNITED STATES DISTRICT COURT

FEB 05 2024

for the

Northern District of Oklahoma

Mark C. McCart, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of
Information Associated with Facebook username
EVAN.PAYTON.18 that is Stored at a Premises
Controlled by Meta Platforms, Inc.

Case No.

24-mj-87-PJC
FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).
located in the Northern District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §924(o)

- Firearms Conspiracy.

The application is based on these facts:

See Affidavit of Special Agent Rebecca Davison, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Subscribed and sworn to by phone.

Date:

2/5/2024City and state: Tulsa, OklahomaR. DAWSON

Applicant's signature

Special Agent Rebecca Davison, ATF

Printed name and title

Judge's signature

Paul Cleary, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH
OF: INFORMATION ASSOCIATED
WITH META PLATFORMS, INC:
FACEBOOK USERNAME
EVAN.PAYTON.18 THAT IS
STORED AT A PREMISES
CONTROLLED BY META
PLATFORMS, INC.

Case No. _____

FILED UNDER SEAL

Affidavit in Support of an Application for a Search Warrant

I, Rebecca Davison, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with the account: Facebook Username **evan.payton.18**, that is stored at a premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), an electronic communications service and/or remote computing service provider headquartered at 1 Meta Way in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government information (including the content of communications) in its possession, pertaining to the subscriber or customer associated with the account: Facebook Username **evan.payton.18**, as further described in Section I of Attachment B. Upon receipt of the

information described in Section I of Attachment B, government-authorized persons will review the information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) within the meaning of 18 U.S.C. § 3051, and as such, am an officer of the United States who is authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. I have been employed by ATF since December 2020. In 2021, I completed the Criminal Investigator Training Program required by the ATF to be an ATF criminal investigator. I also completed the Special Agent Basic Training Academy required by ATF for all special agents employed by ATF. In connection with my official duties as an ATF Special Agent, I investigate criminal violations of federal firearms laws, federal explosives laws, and federal narcotics laws. I have further worked alongside other experienced investigators in relation to firearms and narcotics investigations.

3. Based on my training and experience, I know that it is a violation of Title 18 U.S.C. § 924(o) for any person to conspire to commit a crime of violence.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of

establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

Jurisdiction

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

6. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the government may obtain an order precluding Meta from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Meta Background

7. Meta owns and operates Facebook, a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

8. Meta asks Facebook users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

9. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

10. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other

account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

11. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

12. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can “tag” other Facebook users in a photo or video and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

13. Facebook users can use Facebook Messenger to communicate with other users via text, voice, and video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats, including the date of each call. Facebook users can also

post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

14. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

15. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

16. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

17. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

18. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

19. In addition to the applications described above, Meta provides users with access thousands of other applications (“apps”) on the Facebook platform. When a Facebook

user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

20. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user's IP address is retained by Meta along with a timestamp.

21. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables "Location History," "checks-in" to an event, or tags a post with a location.

22. Social networking providers like Meta typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Meta typically retains records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

23. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish

and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information

indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

24. Therefore, Meta's servers are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

25. I previously requested that Meta preserve any information for the account listed in Attachment A for the time period May 30, 2023 to June 13, 2023.

Probable Cause

26. On June 6, 2023, Tulsa Police Department (TPD) responded to a shooting at the Polo Club Apartments located at 12703 E. 40th Street, in Tulsa, Oklahoma, within the Northern District of Oklahoma. Upon arrival, officers found E'Mari STANCLE on the ground, bleeding from multiple gunshot wounds. EMSA quickly transported STANCLE to Saint Francis Hospital in Tulsa, where medical personnel determined that he had been shot six (6) times, specifically in his abdomen, shoulder, arm, both legs, and upper chest. Next to where officers found STANCLE, they located a Glock model 43X .9mm handgun bearing serial number BWVH553 with a spent .9mm shell casing in the chamber. The firearm had a magazine inserted and contained three (3) .9mm rounds. At the scene, witnesses described a male wearing a white tank top, light blue pants, and a pulled down ski mask, armed with a handgun, walking through the complex shortly after the shooting. TPD officers spotted Evan PAYTON walking in the apartment complex

wearing a white tank top, light blue pants, and a black ski mask. They detained PAYTON because he matched the description given by witnesses. TPD transported an eyewitness who confirmed PAYTON as the person involved in the shooting. PAYTON waived his *Miranda*-rights and officers confirmed his basic information and that he is an enrolled member of the Muscogee Creek Nation. TPD officers did not find a firearm on or near PAYTON when taking him into custody.

27. Officers transported PAYTON to TPD where they conducted a post-*Miranda* interview. PAYTON stated STANCLE, also known as "Snoop", had problems with an individual known as "G-Money." He said "G-Money" and STANCLE were family but did not know the exact relation. He told officers that "G-Money" had a Facebook Username of "G-money Maf Lamont" and an individual he knows as "BG" had a Facebook Username of "BG Maf Lamont." Detectives were able to identify "G-Money" as Gerald MAXWELL and "BG" as Gervorise WARRIOR. PAYTON stated he was in WARRIOR's vehicle with WARRIOR before the shooting. PAYTON told officers that WARRIOR had been trying to get PAYTON to set STANCLE up for a while. PAYTON did not know why WARRIOR wanted to set STANCLE up, only that WARRIOR wanted to "get" STANCLE. PAYTON told officers that he did not want WARRIOR and STANCLE to cross paths. PAYTON said WARRIOR was supposed to leave and "do his own thing" while PAYTON bought the pills from STANCLE. PAYTON stated he planned to text WARRIOR after he finished purchasing pills from STANCLE to pick him up. PAYTON said he did not know that WARRIOR and MAXWELL were planning

to rob STANCLE. He told officers that he did not know STANCLE had a firearm until he pulled it out from under his leg immediately before the shooting. PAYTON denied agreeing to split any stolen items from the robbery with WARRIOR or MAXWELL.

28. At the scene, officers found a silver LG cell phone found in the parking lot near STANCLE's vehicle. PAYTON identified the cell phone as his. He gave TPD investigators consent to view his cell phone. On his phone, investigators found Facebook messages between PAYTON and MAXWELL from June 6, 2023. At approximately 1150 hours, PAYTON messaged MAXWELL that "everything was ready," and they "planned to meet 'him' tonight," referring to STANCLE. At approximately 1228 hours, PAYTON asked what WARRIOR said, and MAXWELL responded they were "going to get shit together and slide down," meaning MAXWELL and WARRIOR were on their way. Shortly after this, PAYTON sent a screenshot of a text conversation he had with STANCLE at phone number (918) 691-9816 to MAXWELL. In that message, PAYTON said he wanted to buy pills from STANCLE. At approximately 1318 hours, he told MAXWELL that STANCLE was "going to pull up for sure" and to "let him know when they were heading there."

29. At approximately 1343 hours, PAYTON told MAXWELL to "bring some blues because he wanted some," referring to pills. MAXWELL replied that he *"didn't know where to get any besides what they were about to do."* PAYTON responded that *"they were about to get some money."* The conversation continued and at approximately 1522 hours,

PAYTON sent MAXWELL his address, 1516 W. Indianola St. Broken Arrow, Oklahoma. Shortly after this, MAXWELL said he "was outside," meaning he picked PAYTON up at his home in Broken Arrow. At approximately 1720 hours, PAYTON messaged that "'he' was there but was backed in," referring to STANCLE. It should be noted that security video showed STANCLE's vehicle was backed into a parking spot when the shooting happened, and this conversation occurred about seven minutes before the shooting.

30. TPD recovered surveillance video of the shooting from a neighbor at the Polo apartments. This video showed an unknown black male wearing jeans and a black shirt approach STANCLE's vehicle with a rifle. While the unknown male is approaching the vehicle, gunshots can be seen coming from the driver's side window of STANCLE's vehicle. After the initial shooting, the unknown male takes cover behind the rear of a van parked near STANCLE's vehicle. The unknown male then shoots multiple rounds into the driver's side of STANCLE's vehicle. After this second round of fire, a person matching PAYTON's description exits STANCLE's vehicle from the front passenger door and flees into the apartment complex. The unknown male then flees the scene, running to a dark colored sedan, jumping in the back, and leaving the area. The video then shows STANCLE's exit the back passenger door of his vehicle, limping, and armed with a pistol. He runs towards the direction TPD later located STANCLE. TPD detectives found multiple 7.62x39mm rifle casings around the van where the unknown shooter took cover.

31. At the scene, TPD found STANCLE's vehicle, a black Hyundai Sonata bearing OK license plate NPX659. The Hyundai had numerous bullet holes and multiple shot out windows. TPD had the vehicle towed to a secured storage location where they executed a Tulsa County search warrant on June 15, 2023. During their search of the vehicle, officers found a black AT&T flip style cell phone with a blue AT&T logo in the center cup holder, multiple .9mm spent shell casings, the same caliber as the Glock43 TPD recovered near to STANCLE, throughout the interior of the vehicle, approximately \$2,662 dollars in U.S. currency in the center console, and approximately 62 round blue pills stamped 'M 30' in two separate plastic baggies in the driver's side door. TPD Forensic Laboratory analyzed the pills and determined they contained fentanyl.

32. ATF SA Rebecca Davison obtained a Northern District of Oklahoma search warrant for the AT&T flip phone from STANCLE's vehicle. 2023-MJ-556-CDL. PAYTON used phone number (918) 822-7666 to message STANCLE at phone number (918) 691-9816. STANCLE's number matched the AT&T flip phone. On June 5 and 6, 2023, PAYTON told STANCLE he was "trying to give him some money and squash their petty beef" and that he "wanted to buy a 'pack.'" Based off my training and experience, a "pack" refers to a "K-Pack" which is a thousand pills, typically fentanyl. STANCLE asked what was up with the money he disputed, and that PAYTON "quit talking to him over some bullshit." PAYTON said that he cashed a check, then asked if STANCLE wanted to meet because he "needed some." They agreed to meetup and STANCLE told PAYTON he was "coming to the side." PAYTON attempted to call STANCLE, but

STANCLE said his phone wasn't letting him answer at 1725 hours. STANCLE made four (4) phone calls to PAYTON from 1720 to 1725 hours. There were no further messages between the two. The shooting occurred roughly two minutes later.

Information to be Searched and Things to be Seized

33. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

34. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

35. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure.

Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any searched keywords.

Conclusion

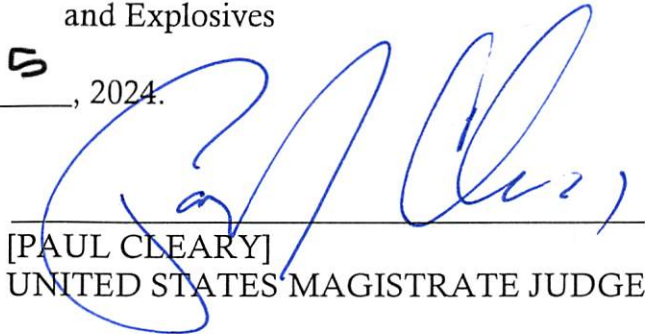
36. Based on the information above, I submit that there is probable cause to believe that there is evidence of violations of Title 18 U.S.C. § 924(o) for any person to conspire to commit a crime of violence, associated with the Facebook account described in Attachment A.

Respectfully submitted,



Rebecca Davison
Special Agent
Bureau of Alcohol, Tobacco, Firearms,
and Explosives

Subscribed and sworn to on February ⁵____, 2024.



[PAUL CLEARY]
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the account: Facebook Username **evan.payton.18**, that is stored at a premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered at 1 Meta Way, Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
2. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected

“Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;

3. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);
4. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
5. All IP logs, including all records of the IP addresses that logged into the account;
6. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
7. Privacy and account settings, including change history, including privacy settings for individual posts and activities, and all records showing which users have been blocked by the account;
8. All past and present lists of friends created by the account;
9. The types of service utilized by the user;

10. All associated logs and metadata;
11. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;

B. All content, records, and other information relating to communications sent from or received by the Account from **May 30, 2023 – June 13, 2023**, including but not limited to:

1. The content of all communications sent from or received by the Account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content, if available;
2. All activity logs for the account and all other documents showing the user's posts and other Facebook activities from **May 30, 2023 – June 13, 2023**.
3. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from **May 30, 2023 – June 13, 2023**, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
4. All other records and contents of communications and messages made or received by the user from **May 30, 2023 – June 13, 2023**, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
5. All "check ins" and other location information;

6. All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken;

C. All content, records, and other information relating to all other interactions between the Account and other users from **May 30, 2023 – June 13, 2023**, including but not limited to:

1. All records of the account's usage of the "Like" feature, including all Facebook and Instagram posts and all non-Facebook webpages and content that the user has "liked";
2. All information about the user's access and use of Facebook Marketplace;
3. All information about the Facebook pages that the account is or was a "fan" of;

D. All records of Facebook and Instagram searches performed by the account from **May 30, 2023 – June 13, 2023**;

E. All location information, including location history, login activity, information geotags, and related metadata from **May 30, 2023 – June 13, 2023**.

F. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows,

followed hashtags, shares, invitations, and all associated logs and metadata, from **May 30, 2023 – June 13, 2023**.

II. Information to be searched for and seized by the government

All information described above in Section I that constitutes evidence and/or fruits of violations of Title 18 U.S.C. § 924(o) for any person to conspire to commit a crime of violence, involving Evan PAYTON and including, for each account or identifier listed on Attachment A:

- a. Communications between the user ID and others from **May 30, 2023 – June 13, 2023**;
- b. Evidence indicating how and when the Facebook and Instagram account were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- c. Evidence indicating the Facebook and Instagram account owner's state of mind as it relates to the crime under investigation;
- d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

Certificate of Authenticity of Domestic Records Pursuant to Federal Rules of Evidence 902(11) and 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Meta Platforms, Inc. (“Meta”) and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Meta. The attached records consist of _____ megabytes of records associated with the Facebook account Facebook Username **evan.payton.18**. I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Meta, and they were made by Meta as a regular practice; and

b. Such records were generated by Meta’s electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Meta in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Meta, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature